Serviciu de validare a semnăturilor digitale în conformitate cu standardele ETSI

- referat – stagiu practică II

coordonator-științific: Mihai-Lică PURA

autor: Ștefan BODOARCĂ

Contents

Introducere

Referat I – stagiu practică: pe lângă o introducere succintă în domeniul semnăturilor digitale și prezentarea importanței standardelor în general și în particular în domeniul anterior amintit, s-a prezentat protocolul de validare a semnăturilor digitale definit de ETSI TS 119 442 [1] și raportul de validare a semnăturii definit de ETSI TS 119 102-2 [2]. Reamintim că acest protocol permite solicitarea validării (și optional augmentarea) și returnează rezultatul validării (și semnătură sporită atunci când este cazul) pentru următoarele tipuri de semnături digitale:

- semnături CMS
- semnături PDF
- semnături XML
- semnături CadES în conformitate cu ETSI EN 319 122, ETSI TS 101 733 sau ETSI TS 103 173
- semnături PadES în conformitate cu ETSI EN 319 142, ETSI TS 102 778 sau ETSI TS 103 172
- semnături XadES în conformitate cu ETSI EN 319 132, ETSI TS 101 903 sau ETSI TS 103 171.

În prezentul document se dorește prezentarea unui exemplu practic de semnare și validare a semnăturilor digitale folosind DSS Web App [3]. Codul sursă al aplicației poate fi găsit la [4].

Framework-ul standardelor publicate pentru domeniul semnăturilor digitale

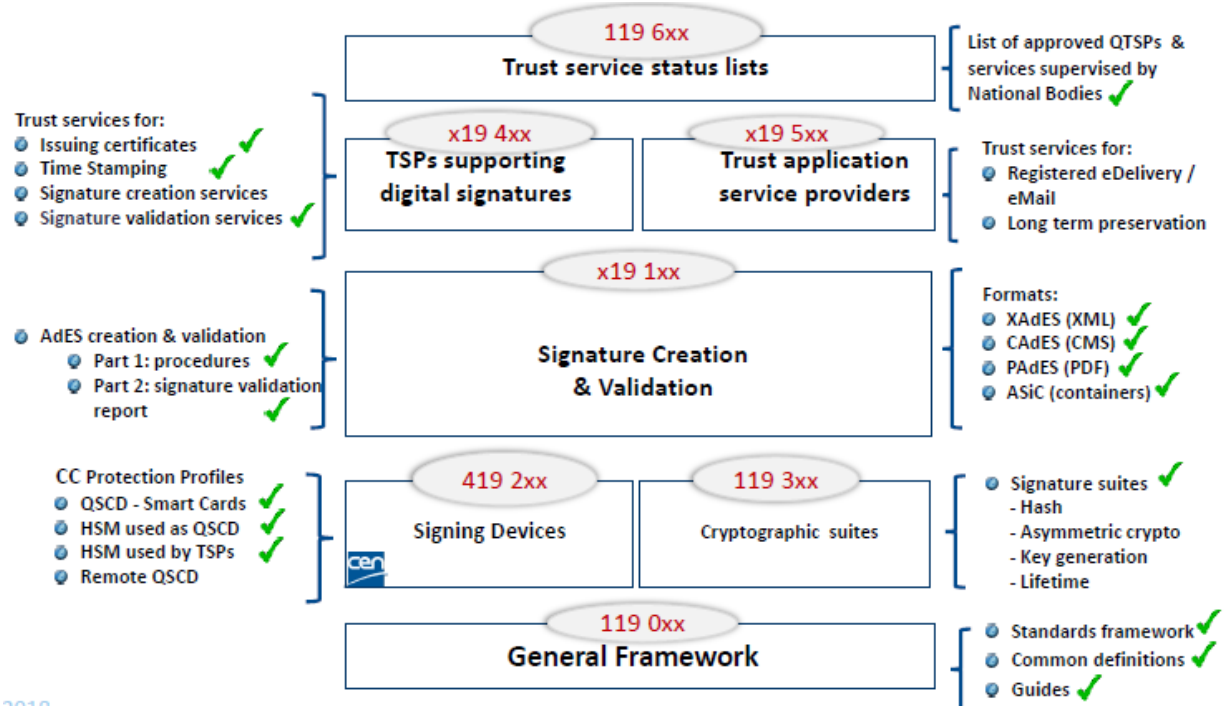

Fig. 1

De interes pentru tema abordată, în ceea ce privește strict validarea semnăturilor digitale, sunt următoarele standarde:

- ETSI TS 119 441 [5] – Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services – în care sunt expuse politicile pe care un furnizor de servicii de încredere (eng. Trust Service Provider) trebuie să le respecte pentru a putea oferi servicii de validare a semnăturii
- ETSI TS 119 442 [1] - Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services – în care este definit un protocol ce permite unui client să solicite validarea sau validarea și augmentarea semnăturilor digitale la un server de la distanță și permite serverului să returneze rezultatul validării clientului solicitant și, la cerere, semnătura să fie sporită în consecinţă.
- ETSI TS 119 102-1 [6] - Electronic Signatures and Infrastructures (ESI);Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation – în care este descris mecanismul de creare și validare a semnăturilor
- ETSI TS 119 102-2 [2] - Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report – în care se prezintă formatul și semnificația raportului de validare a semnăturii.

Definire tipuri de semnături suportate

Cryptographic Message Syntax (CMS) este standardul IETF pentru mesaje protejate criptografic. Acest standard poate fi folosit pentru a semna digital, pentru hash-uri criptografice, pentru autentificarea sau criptarea oricăror tipuri de date digitale [8].

CMS se bazează pe sintaxa PKCS#7, care, la rândul său, se bazează pe standardul Privacy-Enhanced Mail. Cea mai recentă versiune de CMS este specificată în RFC 5652 [7].

Arhitectura CMS este construită în jurul managementului de chei din certificatele digitale, cum ar fi profilul definit de grupul de lucru PKIX.

CMS este folosit ca o componentă criptografică de bază pentru multe alte standarde criptografice, cum ar fi S/MIME, PKCS#12 și protocolul de timestamp RFC 3161.

CAdES (CMS Advanced Electronic Signatures) reprezintă o extensie a CMS astfel încât CMS să fie potrivit pentru semnături AdES (advanced electronic signature).

O semnătură electronică avansată (AdES) este o semnătură electronică care îndeplinește cerințele stabilite în temeiul Regulamentului UE nr. 910/2014 (regulamentul eIDAS) privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă [9].

PAdES (PDF Advanced Electronic Signatures) reprezintă o extensie a datelor semnate PDF astfel încât să fie potrivite pentru semnături AdES (advanced electronic signature) [10].

Semnătura XML (denumită și XMLDSig, XML-DSig, XML-Sig) definește o sintaxă XML pentru semnăturile digitale și este definită în recomandarea W3C XML Signature Syntax and Processing. Funcțional, acesta are multe în comun cu PKCS#7, dar este mai ușor de extins și este orientată spre semnarea documentelor XML. Semnătura XML este folosită de diferite tehnologii web, cum ar fi SOAP, SAML și altele [11].

Semnăturile XML pot fi folosite pentru a semna date - o resursă - de orice tip, de obicei documente XML, dar orice poate fi accesibil printr-un URL poate fi semant. O semnătură XML folosită pentru a semna o resursă aflată în afara documentului XML care conține semnătura este numită semnătură detașată; dacă este folosită pentru a semna o parte din documentul care conține semnătura se numește semnătura anvelopată; dacă semnătura conține datele semnate în sine, se numește o semnătură care anvelopează [11].

XAdES (XML Advanced Electronic Signatures) reprezintă o extensie a recomandării XML-DSig, astfel încât semnăturile să fie potrivite pentru AdES (advanced electronic signature). W3C și ETSI mențin și actualizează împreună XAdES. [13].

Exemplu de semnare și validare folosind DSS Web App

1. Creare CA cu certificat auto-semnat

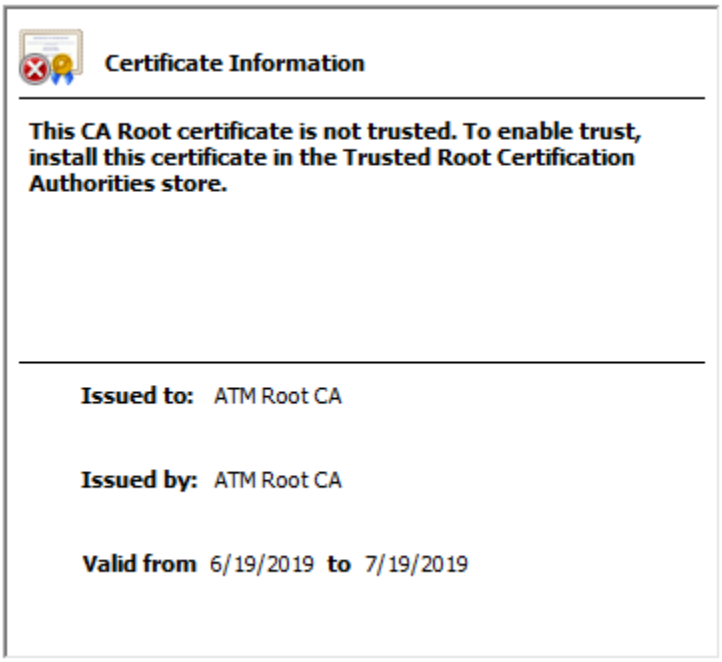

Fig. 2

2. Creare certificat pentru un sever și semnarea acestuia de către ATM Root CA

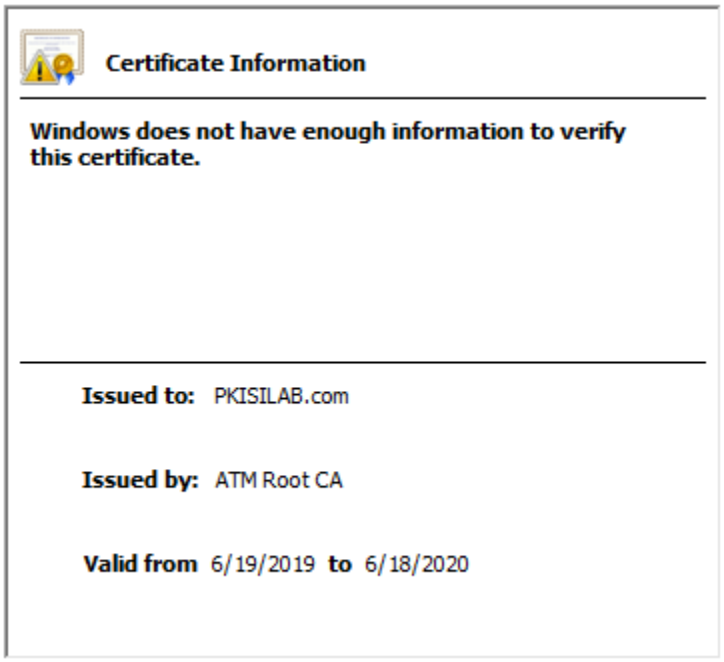

Fig. 3

3. Se semnează un PDF cu o semnătură normală PDF și un alt PDF cu o semnătură PAdES

Fig. 4

Fig. 5 Interfață semnare pdf DSS Web APP

4. Validare semnăturii și obținerea raportului de validare

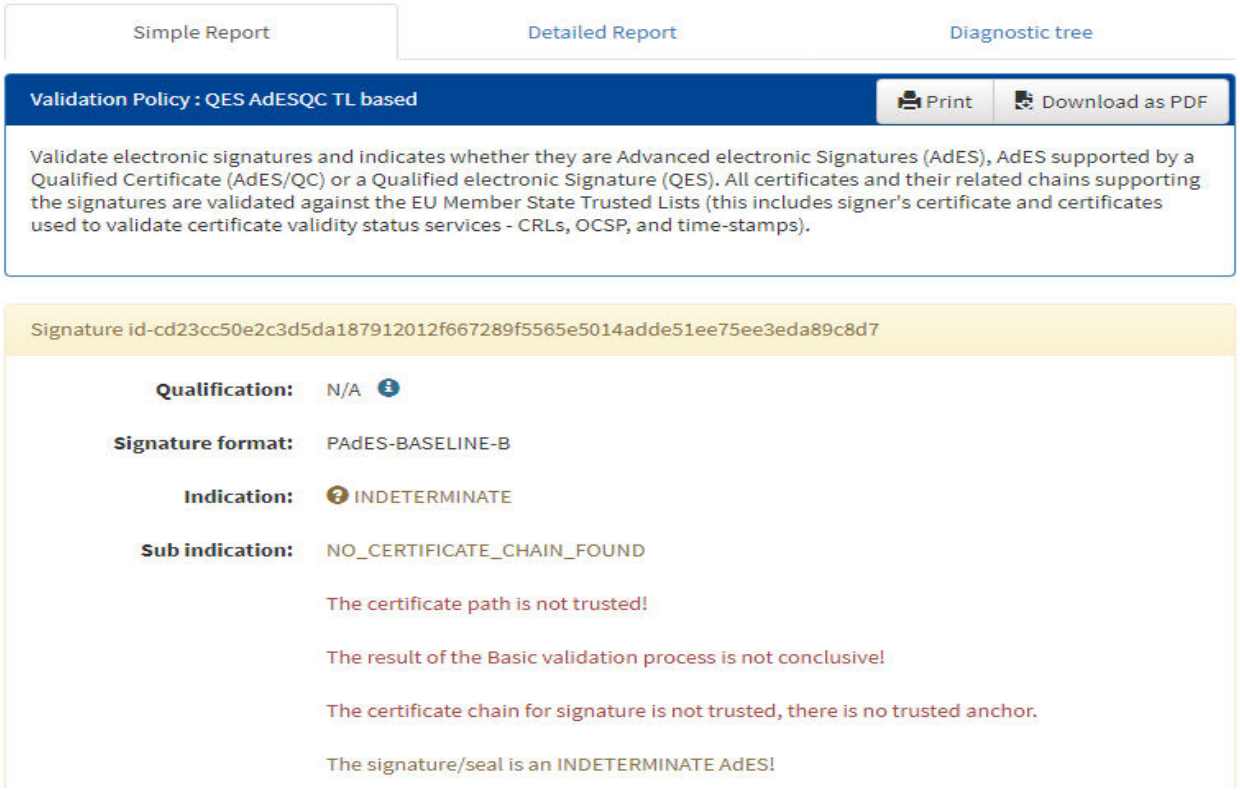

Fig. 6 Raport simplu

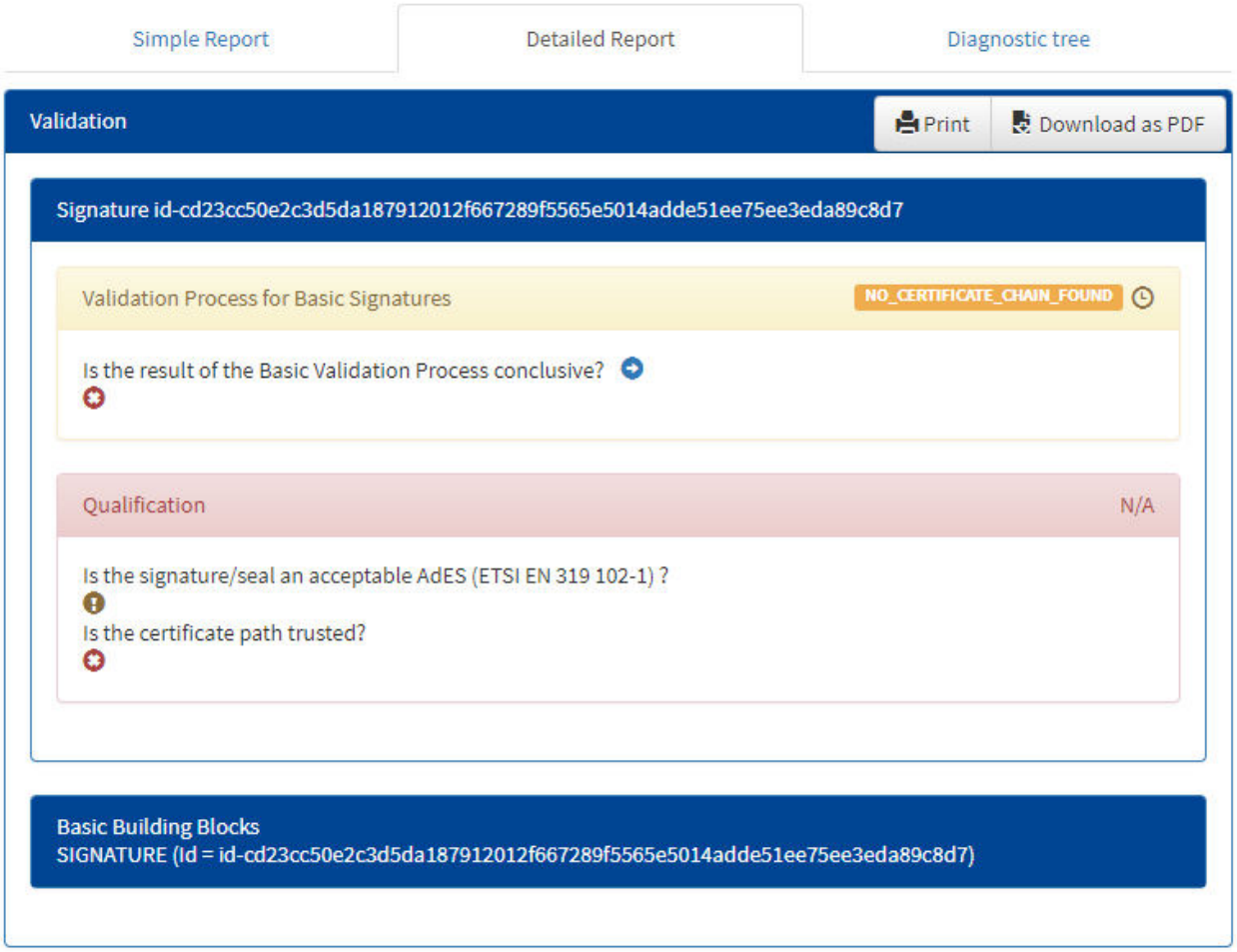

Fig. 7

Rezultat: nedeterminat datorită faptului că lanțul de certificare nu e trusted

Informațiile de validare raportate		Semnificație
Status indicat	Datele care apar în raport	
TOTAL-PASSED	Procesul de validare ar trebui să afișeze lanțul de încredere, incluzând certificatul cu care s-a semnat și care a fost folosit în procesul de validare. Mai mult, procesul de validare poate oferi rezultate ale validării pentru fiecare constrângere de validare în parte. Procesul de validare ar trebui să ofere pentru DA (eng. driving application) access la atributele semnate prezente în semnătură, respectiv la identitatea semnatarului.	Rezultatul validării este TOTAL-PASSED dacă: • verificarea formatului a reușit; • verificarea criptografică a semnăturii a reușitș • orice constrângere aplicabilă certificatului semnatarului a fost pozitiv validatăș • semnătura a fost pozitiv validată față de constrângerile de validare;
TOTAL-FAILED	Procesul de validare trebuie să ofere informații adiționale pentru a explica statusu-ul de TOTAL-FAILED pentru fiecare constrângere care a fost luată în considerare și care a dus la un rezultat negativ.	Procesul de validare se termină cu TOTAL-FAILED deoarece verificarea de format a eșuat, verificările criptografice pe semnătură au eșuat sau s-a demonstrat că certificatul era invalid la momentul semnării.
INDETERMINATE	Procesul de validare trebuie să ofere informații suplimentare pentru a explica rezultatul de INDETERMINATE, astfel încât cel care realizează validarea să poată identifica ce date lipsesc pentru a completa procesul de validare. În particular, trebuie să ofere rezultatul validării pentru acele constrângeri care au fost luate în considerare și pentru a rezultatul a fost	Informația valabilă nu este suficientă pentru a stabili rezultatul de TOTAL-PASSED sau TOTAL-FAILED.

	‚indeterminate'.	

Tabel 1 [6]

Procesul de validare

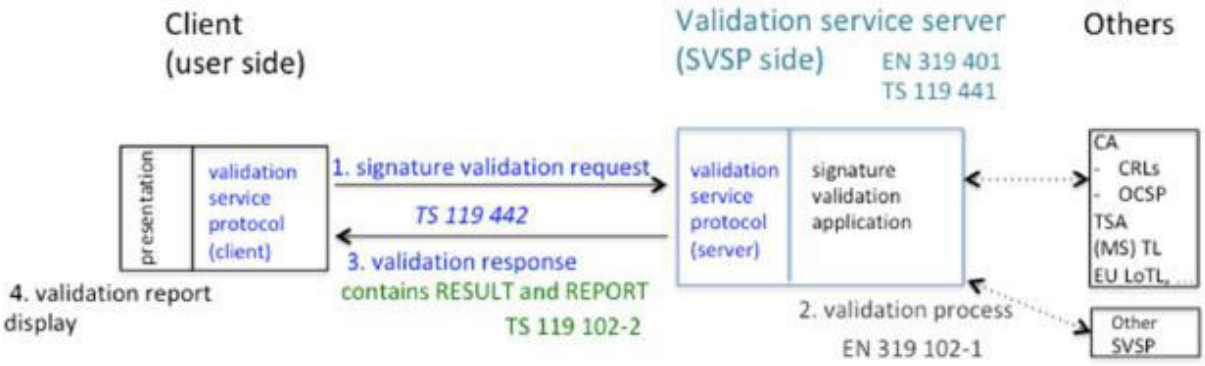

Fig. 8

1. Clientul generează și trimite o cerere de validare a semnăturii.

Cererea include:

- documentul semnat și semnătura sau
- o reprezentare a documentului semnat și semnătura, pentru a evita expunerea documentului către serviciul de validare
- (opțional) constrângeri de validare ale certificatelor și timestamp-uri, acestea două reprezentând componente ale semnăturii ce urmează să fie validată după cum este specificat în ETSI TS 102-1.

2. SVSServ (Signature Validation Service Server) realizează procesul de validare

Procesul de validare este specificat în ETSI TS 119 102-1. Validarea este realizată de către SVSP (Signature Validation Service Provider) conform constrângerilor care pot fi oferite de client sau de serviciul în sine:

- dacă mulțimea de constrângeri nu este oferită de client, SVS (Signature Validation Service) poate implementa o politică implicită de validare
- dacă mulțimea de constrângeri este oferită de client, atunci poate fi completată politica de validare a semnăturii, după cum cer practicile SVSP

3. SVSServ pregătește și trimite răspunsul validării

4. Prezentarea raportului de validare

Aplicația client prezintă raportul de validare și orice alte informații relevante. Bazându-se pe raportul de validare (ex. rezultat ‘indeterminate’), utilizatorul poate să accepte sau nu semnătura.

Bibliografie

[1] https://www.etsi.org/deliver/etsi_ts/119400_119499/119442/01.01.01_60/ts_119442v010101p.pdf

[2] https://www.etsi.org/deliver/etsi_ts/119100_119199/11910202/01.01.01_60/ts_11910202v010101p.pdf

[3] https://ec.europa.eu/cefdigital/DSS/webapp-demo/

[4] https://github.com/esig/dss

[5] https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf

[6] https://www.etsi.org/deliver/etsi_ts/119100_119199/11910201/01.02.01_60/ts_11910201v010201p.pdf

[7] https://tools.ietf.org/html/rfc5652

[8] https://en.wikipedia.org/wiki/Cryptographic_Message_Syntax

[9] https://en.wikipedia.org/wiki/Advanced_electronic_signature

[10] https://en.wikipedia.org/wiki/PAdES

[11] https://en.wikipedia.org/wiki/XML_Signature

[12] https://en.wikipedia.org/wiki/XAdES

[13] https://en.wikipedia.org/wiki/XAdES